DOI: 10.1155/2019/2108014

Hindawi
Complexity
Volume 2019, Article ID 2108014, 13 pages
https://doi.org/10.1155/2019/2108014

Research Article

Binomial Representation of Cryptographic Binary Sequences and Its Relation to Cellular Automata

Sara D. Cardell [1] **and Amparo Fúster-Sabater** [2]

[1] *IMECC, University of Campinas (UNICAMP), Brazil*
[2] *Institute of Physical and Information Technologies, C.S.I.C., Madrid, Spain*

Correspondence should be addressed to Sara D. Cardell; sdcardell@ime.unicamp.br

Received 23 December 2018; Accepted 13 February 2019; Published 24 March 2019

Academic Editor: Jose C. Valverde

The binomial sequences are binary sequences that correspond to the diagonals of the binary Sierpinski's triangle. They have fancy properties such that all the sequences with period equal to a power of 2 can be represented as the sum of a finite set of binomial sequences. Other structural properties of these sequences (period, linear complexity, construction rules, or relations among the different binomial sequences) have been analyzed in detail. Furthermore, this work enhances the close relation between the binomial sequences and a kind of Boolean networks, known as linear cellular automata. In this sense, the binomial sequences exhibit the same behavior as that of particular Boolean networks. Consequently, the binomial sequences can be considered as primary tools for generating other more complex Boolean networks with applications in communication systems and cryptography.

1. Introduction

Pseudorandom binary sequences are simple successions of bits with applications in fields so different as spread-spectrum communications, circuit testing, error-correcting codes, numerical simulations, or cryptography (stream cipher). Most generators producing such sequences are based on Boolean functions and Linear Feedback Shift Registers (LFSRs) [1]. Desirable characteristics for pseudorandom binary sequences are long period, good statistical properties or large linear complexity. Different LFSR-based sequence generators can be found in the literature [2, Chapter 5]. In most of them, the output sequence is a binary sequence generated as the image of a nonlinear Boolean function in the shift register binary stages.

On the other hand, the binomial sequences are a family of binary sequences whose terms are binomial numbers reduced modulo 2. More precisely, the binomial sequences correspond to the diagonals of the Sierpinski's triangle modulo 2. In this way, the binomial sequences exhibit many attractive properties that can be very useful in the analysis and generation of cryptographic sequences. In this work, it is shown that every binary sequence with period 2^L, L being a positive integer, can be written as a bit-wise XOR of binomial sequences.

Since many of the cryptographic sequences have period 2^L [3–6], then the binomial sequences can be considered as a fundamental tool to analyze the structural properties of all these classes of sequences. In addition, it can be checked that the behavior of some binomial sequence combinations is the same as that of a kind of Boolean networks (namely, one-dimensional cellular automata). In fact, cellular automata with two-state cells is a special kind of Boolean network where all the nodes use the same function and the links are all arranged in a regular bounded integer lattice structure. Boolean networks have attracted great attention in many different areas such as bioinformatics [7], computational processes [8], graph dynamical systems [9], and parallel discrete dynamical systems [10, 11]. This paper shows the subtle relation between binomial sequences and cellular automata. In brief, the binomial sequences and the linear cellular automata make visible the linearity inherent to many cryptographic generators paradoxically designed as strong nonlinear generators.

The paper is organized as follows: In Section 2, we introduce the basic concepts and definitions needed for the rest of this work. Section 3 studies the characterization and main properties of the binomial sequences. In Section 4, the relation between binomial sequences and linear cellular automata is analyzed. A simple method of recovering the binomial representation of a sequence is developed in Section 5 with an example. Finally, conclusions in Section 6 end the paper.

2. Preliminaries

In this section, we present some basic concepts about sequences that we need to know before introducing the main results.

2.1. Binary Sequences. Let $\mathbb{F}_2$ be the Galois field of two elements. We say $\{a_n\} = \{a_0, a_1, a_2 \ldots\}$ is a binary sequence if its terms $a_n \in \mathbb{F}_2$, for $n = 0, 1, 2, \ldots$. The sequence $\{a_n\}$ is periodic if and only if there exists an integer T such that $a_{n+T} = a_n$, for all $n \geq 0$. In the sequel, all the sequences considered will be binary sequences and the XOR operation among sequences will be denoted by + instead of the symbol $\oplus$.

Let r be a positive integer, and let $d_1, d_2, d_3, \ldots, d_r$ be constant coefficients with $d_i \in \mathbb{F}_2$. A binary sequence $\{a_n\}$ satisfying the relation

$$a_{n+r} = d_r a_n + d_{r-1} a_{n+1} + \cdots + d_3 a_{n+r-3} + d_2 a_{n+r-2} + d_1 a_{n+r-1}, \quad n \geq 0, \tag{1}$$

is called a (r-th order) linear recurring sequence in $\mathbb{F}_2$. The terms $\{a_0, a_1, \ldots, a_{r-1}\}$ are referred to as the initial values (or initial state) and determine the rest of the sequence uniquely. A relation of the form given by (1) is called a (r-th order) linear recurrence relationship.

The monic polynomial

$$p(x) = d_r + d_{r-1} x + \cdots + d_3 x^{r-3} + d_2 x^{r-2} + d_1 x^{r-1} + x^r \in \mathbb{F}_2[x] \tag{2}$$

is called the characteristic polynomial of the linear recurring sequence and $\{a_n\}$ is said to be generated by $p(x)$.

The generation of linear recurring sequences can be implemented on LFSRs [1]. These structures handle information in the form of binary elements and they are based on shifts and linear feedback. In fact, an LFSR is an electronic device with r memory cells (stages) with binary contents. At each time instant, each element is shifted to the adjacent stage and a new element is computed via a linear feedback to fill the empty stage (see Figure 1). If the characteristic polynomial of the linear recurring sequence is primitive [1], then the LFSR is a maximal-length LFSR and its output sequence, the so-called PN-sequence, has period $T = 2^r - 1$.

The linear complexity, LC, of a sequence $\{a_n\}$ is defined as the length of the shortest LFSR that generates such a sequence or, equivalently, as the lowest order linear recurrence relationship that generates such a sequence.

In cryptographic terms, the linear complexity must be as large as possible. The recommended value is approximately half the period $LC \simeq T/2$.

Let E be the shifting operator that acts on the terms of a sequence $\{a_n\}$; that is,

$$E^k a_n = a_{n+k}, \quad \text{for all integer } k \geq 0. \tag{3}$$

The linear recurrence relationship given in (1) can be written in terms of the operator E as a linear difference equation:

$$\left(E^r + \sum_{j=1}^{r} d_j E^{r-j}\right) a_n = 0, \quad \text{for } n \geq 0. \tag{4}$$

If the characteristic polynomial $p(x)$ is a primitive polynomial of degree r and $\alpha \in \mathbb{F}_{2^r}$ is one of its roots, then $\alpha, \alpha^2, \alpha^{2^2}, \ldots, \alpha^{2^{r-1}}$ are the r roots of such a polynomial. In this case, the binary solutions of (4) are a linear combination of the r roots of the form

$$a_n = \sum_{j=0}^{r-1} c_i^{2^j} \alpha^{2^j n}, \tag{5}$$

that is, a_n is the n-th term of a PN-sequence with characteristic polynomial $p(x)$ and whose initial values are determined by the coefficient $c_i \in \mathbb{F}_{2^r}$.

Next, let us consider a bit more complex difference equation of the form

$$\left(E^r + \sum_{j=1}^{r} d_j E^{r-j}\right)^m z_n = 0, \quad \text{for } n \geq 0, \tag{6}$$

whose characteristic polynomial is $p_m(x) = p(x)^m = (x^r + \sum_{j=1}^{r} d_j x^{r-j})^m$, m being a positive integer. Now, the roots of $p_m(x)$ are the same as those of $p(x)$ but with multiplicity m. Therefore, the binary solutions of (6) are given by

$$z_n = \sum_{i=0}^{m-1} \left[\binom{n}{i} \sum_{j=0}^{r-1} c_i^{2^j} \alpha^{2^j n} \right], \tag{7}$$

where the coefficients $c_i \in \mathbb{F}_{2^r}$ and $\binom{n}{i}$ are binomial coefficients reduced modulo 2 (see [12]). Since

$$\sum_{j=0}^{r-1} c_i^{2^j} \alpha^{2^j n} \tag{8}$$

is the n-th term of a PN-sequence with characteristic polynomial $p(x)$ and initial values determined by c_i, then z_n is the sum of m terms of a unique PN-sequence starting at different points and where each one of these m terms is weighted by a binary binomial coefficient $\binom{n}{i}$.

Table 1: Binomial sequences, first eight terms, period, and linear complexity.

Binomial coeff.	Binomial sequences	Period	Linear complexity
$\binom{n}{0}$	1 1 1 1 1 1 1 1	$T_0 = 1$	$LC_0 = 1$
$\binom{n}{1}$	0 1 0 1 0 1 0 1	$T_1 = 2$	$LC_1 = 2$
$\binom{n}{2}$	0 0 1 1 0 0 1 1	$T_2 = 4$	$LC_2 = 3$
$\binom{n}{3}$	0 0 0 1 0 0 0 1	$T_3 = 4$	$LC_3 = 4$
$\binom{n}{4}$	0 0 0 0 1 1 1 1	$T_4 = 8$	$LC_4 = 5$
$\binom{n}{5}$	0 0 0 0 0 1 0 1	$T_5 = 8$	$LC_5 = 6$
$\binom{n}{6}$	0 0 0 0 0 0 1 1	$T_6 = 8$	$LC_6 = 7$
$\binom{n}{7}$	0 0 0 0 0 0 0 1	$T_7 = 8$	$LC_7 = 8$

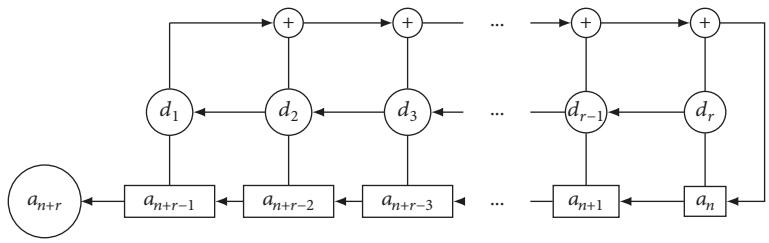


Figure 1: LFSR of length r.

3. Binomial Sequences

Previous to the introduction of the binomial sequence concept, let us consider some general features of the binomial coefficients.

The binomial coefficient $\binom{n}{i}$ is the coefficient of the power x^i in the polynomial expansion of $(1 + x)^n$. For every positive integer n, it is a well-known fact that $\binom{n}{0} = 1$ and $\binom{n}{i} = 0$ for $i > n$. Moreover, it is worth noticing that if we arrange these binomial coefficients into rows for successive values of $n = 0, 1, 2, \ldots$, then the generated structure is the Pascal's triangle (see Figure 2(a)). The most-left diagonal is the identically 1 sequence, the next diagonal is the sequence of natural numbers $\{1, 2, 3, \ldots\}$, the next one is the sequence of triangular numbers $\{1, 3, 6, 10, \ldots\}$, etc. Other fascinating sequences (tetrahedral numbers, pentatope numbers, hexagonal numbers, Fibonacci sequence, etc.) can be found in the diagonals of this triangle. On the other hand, if we color the odd numbers of the Pascal's triangle and shade the even numbers, then we get the Sierpinski's triangle (see Figure 2(b)).

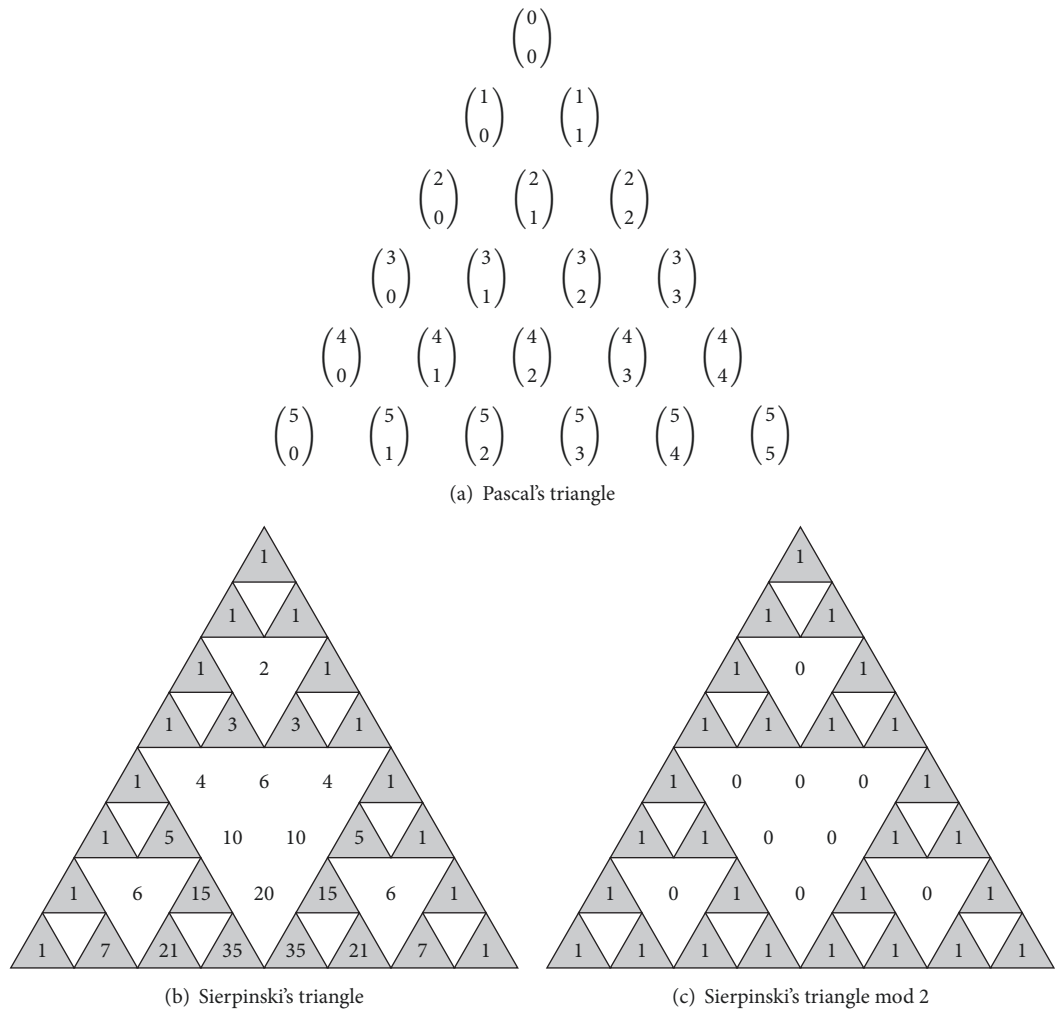
The binomial coefficients reduced modulo 2 allow us to introduce the concept of binomial sequence.

Definition 1. Given a fixed integer $k \geq 0$, the sequence $\{b_n^k\}_{n \geq 0}$ given by

$$b_n^k = \begin{cases} 0 & \text{if } n < k \\ \binom{n}{k} \bmod 2 & \text{if } n \geq k \end{cases} \tag{9}$$

is known as the *binary k-th binomial sequence*.

Table 1 shows the binomial sequences and their corresponding periods and linear complexities, denoted by T_i and LC_i, respectively, for the first 8 binomial coefficients $\binom{n}{i}$, $i = 0, 1, \ldots, 7$; see [12]. The linear complexities of the binomial sequences are defined in Theorem 13 (Section 4). Recall that the successive binomial sequences correspond to shifted versions of the successive diagonals in the Sierpinski's triangle reduced modulo 2 (see Figure 2(c)).



(a) Pascal's triangle

(b) Sierpinski's triangle

(c) Sierpinski's triangle mod 2

Figure 2: Binomial coefficients arranged as triangles.

Next, the relation between binomial sequences and binary sequences with period which is a power of 2 is defined in the following result.

Theorem 2. *Let $\{z_n\}$ be a binary sequence with period $T = 2^L$, L being a positive integer. Then, every binary sequence $\{z_n\}$ can be written as a linear combination of binomial sequences.*

Proof. Since the period of $\{z_n\}$ is a power of 2, then the next equation holds:

$$\left(E^{2^L} + 1\right) z_n = (E+1)^{2^L} z_n = 0, \tag{10}$$

which is a simplified version of (6) with $m = 2^L$ and the characteristic polynomial $p_m(x) = p(x)^m = (x+1)^m$. Therefore, its binary solutions are given by (7), which has now the following simplified form:

$$z_n = \binom{n}{0} c_0 + \binom{n}{1} c_1 + \cdots + \binom{n}{T-1} c_{T-1} \quad \text{for } n \geq 0, \tag{11}$$

where 1 is the unique root of the polynomial $(x+1)^T$ with multiplicity $T = 2^L$, the coefficients $c_i \in \mathbb{F}_2$ and $\binom{n}{i}$ are binomial coefficients modulo 2. When n takes successive values $n = 0, 1, 2, \ldots$, then each binomial coefficient modulo 2 defines a different binomial sequence. Thus, the sequence $\{z_n\}$ is just the bit-wise XOR of such binomial sequences weighted by binary coefficients c_i. □

Different choices of c_i will produce different sequences $\{z_n\}$ with distinct characteristics and properties, but all of them with period 2^l, $0 \leq l \leq L$.

4. Properties of the Binomial Sequences

From now on, we denote the k-th binomial sequence $\{b_n^k\}_{n\geq 0}$ as $\left\{\binom{n}{k}\right\}_{n\geq 0}$ or simply $\left\{\binom{n}{k}\right\}$, while $\binom{n}{k}$ denotes a binomial coefficient.

In this section we study the properties of this family of binomial sequences.

Next result shows that the binomial sequences can be obtained one from another.

Proposition 3. *Given the sequence* $\{\binom{n}{2^L+k}\}$, *with* $0 \le k < 2^L$, *we have that*

(a) *the sequence has period* $T = 2^{L+1}$;

(b) *the first period of the sequence has the following structure:*

$$\left\{\binom{n}{2^L+k}\right\}_{0\le n<2^{L+1}} = \begin{cases} 0 & \text{if } 0 \le n < 2^L + k, \\ \binom{n}{k} & \text{if } 2^L + k \le n < 2^{L+1}. \end{cases} \tag{12}$$

Proof. (b) We consider the first 2^{L+1} bits of the sequence $\{\binom{n}{2^L+k}\}$.

We know that $\binom{n}{2^L+k} = 0$ when $n < 2^L + k$. Then, the first $2^L + k$ bits are 0s; in particular, this means that the first 2^L elements of the sequence are zero.

If $n \ge 2^L + k$, then n is of the form $n = 2^L + k + t$, for $0 \le t < 2^L - k$. We want to prove that the other 2^L bits are the first 2^L bits of $\{\binom{n}{k}\}$. This idea is illustrated in Figure 3.

In order to prove that the other 2^L bits are the first 2^L bits of $\{\binom{n}{k}\}$, it is enough to prove that $\binom{2^L+k+t}{2^L+k} \equiv \binom{k+t}{k} \pmod 2$.

Thus, we compute both binomial coefficients

$$\begin{aligned} \binom{2^L+k+t}{2^L+k} &= \frac{(2^L+k+t)!}{(2^L+k)!t!} \\ &= \frac{(2^L+k+t)\cdots(2^L+k+1)}{t!}, \\ \binom{k+t}{k} &= \frac{(k+t)\cdots(k+1)}{t!} \end{aligned} \tag{13}$$

Let 2^{p_i} be the maximum power of 2 in the prime factorization of $k + i$, with $0 < i \le t$ and q_i the odd number such that $k + i = 2^{p_i} q_i$. Notice that when $k + i$ is odd, then $k + i = q_i$ and $p_i = 0$.

Then, we have

$$\begin{aligned} &\binom{2^L+k+t}{2^L+k} \\ &= \frac{2^{p_t+p_{t-1}+\cdots+p_1}\left(2^{L-p_t}+q_t\right)\left(2^{L-p_{t-1}}+q_{t-1}\right)\cdots\left(2^{L-p_1}+q_1\right)}{t!}, \end{aligned} \tag{14}$$

$$\binom{k+t}{k} = \frac{2^{p_t+p_{t-1}+\cdots+p_1} q_t \cdot q_{t-1}\cdots q_1}{t!} \tag{15}$$

Since $k + i < 2^L$, then $2^{p_i} q_i < 2^L$ and, as a consequence, $p_i < L$. Now, the inequality $L - p_i > 0$ implies that $2^{L-p_i} + q_i$ is always an odd number. Finally, since both (14) and (15) have the same denominator, then they exhibit the same powers of two. Thus, (14) is odd (even) iff (15) is odd (even) and the previous congruence holds.

(a) It is enough to prove now that

$$\binom{2^{L+m}+t}{2^L+k} \equiv \binom{2^{L+m+1}+t}{2^L+k} \bmod 2 \tag{16}$$

We consider both binomial coefficients:

$$\begin{aligned} &\binom{2^{L+m}+t}{2^L+k} \\ &= \frac{\left(2^{L+m}+t\right)\cdot\left(2^{L+m}+t-1\right)\cdots\left(2^{L+m}+t-2^L-k+1\right)}{(2^L+k)!} \\ &\binom{2^{L+m+1}+t}{2^L+k} \\ &= \frac{\left(2^{L+m+1}+t\right)\cdot\left(2^{L+m+1}+t-1\right)\cdots\left(2^{L+m+1}+t-2^L-k+1\right)}{(2^L+k)!} \end{aligned} \tag{17}$$

Consider 2^{p_i} the maximum power of 2 in the prime factorization of i, with $t - 2^L - k + 1 \le i \le t$ and q_i the odd number such that $2^{p_i} \cdot q_i = i$. Notice that when i is odd, then $p_i = 0$ and $i = q_i$. With this new notation, we have that

$$\binom{2^{L+m}+t}{2^L+k} = \frac{2^{p_t\cdot p_{t-1}\cdots p_{t-2^L-k+1}}\left(2^{L+m-p_t}+q_t\right)\cdot\left(2^{L+m-p_{t-1}}+q_{t-1}\right)\cdots\left(2^{L+m-p_{t-2^L-k+1}}+q_{t-2^L-k+1}\right)}{(2^L+k)!} \tag{18}$$

$$\binom{2^{L+m+1}+t}{2^L+k} = \frac{2^{p_t\cdot p_{t-1}\cdots p_{t-2^L-k+1}} q_t \cdot q_{t-1}\cdots q_{t-2^L-k+1}}{(2^L+k)!} \tag{19}$$

Note that $L + m - p_i > 0$ and then $2^{L+m-p_i} + q_i$ is always an odd number. Now, since both expressions (18) and (19) have the same denominator and the same powers of two in the prime factorization of the numerator, we know that (18) is odd (even) iff (19) is odd (even).

We have proven that $\binom{n}{2^L+k} = \binom{n+2^{L+1}}{2^L+k}$, for $n \ge 0$. Then we know that the period divides 2^{L+1}. Since the first 2^L bits of the sequence are 0s (item b), then the period must be $T = 2^{L+1}$. □

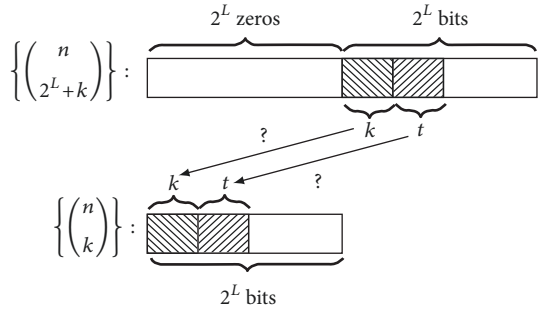


FIGURE 3: Structure of the binomial sequences $\{\binom{n}{k}\}$ and $\{\binom{n}{2^L+k}\}$.

In Figure 8, we can see the structure of the first 32 binomial sequences. It is easy to observe the pattern and the periods mentioned in Proposition 3.

It is worth noticing that the binomial sequences match exactly with the diagonals of the binary Sierpinski's triangle (see Figure 4) but starting in a different bit (shifted versions of such diagonals). For example, the encircled sequence in Figure 4 corresponds to the shifted binomial sequence $\{\binom{n}{4}\}$.

We know that the sequence $\{\binom{n}{k}\}$ is a solution of the difference equation of the form (10). Therefore, every sequence of period 2^L can be obtained by XORing diagonals of the binary Sierpinski's triangle.

Corollary 4. *The sequences* $\{\binom{n}{2^L}\}$ $(L = 0, 1, 2, \ldots)$ *have period* $T = 2^{L+1}$ *and the following structure:*

$$\left\{\binom{n}{2^L}\right\}_{0\le n<2^{L+1}} = \begin{cases} 0 & \text{if } 0 \le n < 2^L, \\ 1 & \text{if } 2^L \le n < 2^{L+1}. \end{cases} \tag{20}$$

Corollary 5. *The sequences* $\{\binom{n}{2^L}\}$ $(L = 0, 1, 2, \ldots)$ *are balanced; that is to say, they contain the same number of 1s and 0s.*

Remark 6. (a) The sequences of the form $\{\binom{n}{2^L}\}$ have the following structure:

$$\underbrace{0\ 0\ \ldots 0}_{2^L \text{ zeros}}\underbrace{1\ 1\ \ldots\ 1}_{2^L \text{ ones}} \tag{21}$$

(b) The sequences of the form $\{\binom{n}{2^L+k}\}$ have the following structure:

$$\underbrace{0\ 0\ \ldots 0}_{2^L \text{ zeros}}\underbrace{\ldots\ldots\ldots\ldots}_{\substack{2^L \text{ first terms} \\ \text{of } \{\binom{n}{k}\}}} \tag{22}$$

According to Theorem 2, a binary sequence of period power of 2 is the bit-wise XOR of binomial sequences. Therefore, we introduce the following definition.

Definition 7. The set of binomial sequences necessary to obtain a binary sequence of period power of 2 is called the *binomial representation* of such a sequence.

The binomial representation of a sequence is of the form $\sum_{i=0}^{M} c_i \{\binom{n}{i}\}$, with $c_i \in \mathbb{F}_2$ and M an integer such that $M \ge 0$.

Since our sequences are periodic, they can start in different points. Next we see that, depending on the starting point, the binomial representations of the same sequence will be different.

Lemma 8. *Given two positive integers* n *and* t *with* $n > t$, *we have the following:*

$$\binom{n}{t} + \binom{n}{t-1} = \binom{n+1}{t} \tag{23}$$

Proof.

$$\begin{aligned} \binom{n}{t} + \binom{n}{t-1} &= \frac{n!}{t!\,(n-t)!} + \frac{n!}{(t-1)!\,(n-t+1)!} \\ &= \frac{(n-t+1)\cdot n! + t\cdot n!}{t!\,(n-t+1)!} \\ &= \frac{(n+1)!}{t!\,(n+1-t)!} = \binom{n+1}{t} \end{aligned} \tag{24}$$

□

Lemma 9. *Given the binomial sequence* $\{\binom{n}{t}\}$, $t \ge 1$, *if we shift cyclically such a sequence one bit to the left, then we obtain the sequence* $\{\binom{n}{t} + \binom{n}{t-1}\}$. *If* $t = 0$, *the sequence remains the same (in this case the sequence is the identically 1 sequence).*

Proof. According to the construction rule for binomial sequences given in Definition 1, the sequences $\{\binom{n}{t}\}$ and $\{\binom{n+1}{t}\}$ are the same but starting in different points.

Now, according to Lemma 8, we know that $\binom{n}{t} + \binom{n}{t-1} = \binom{n+1}{t}$, then the sequence $\{\binom{n+1}{t}\}$ equals the sequence $\{\binom{n}{t} + \binom{n}{t-1}\}$. Therefore, the sequences $\{\binom{n}{t}\}$ and $\{\binom{n}{t} + \binom{n}{t-1}\}$ are the same but starting in different bits. □

Example 10. Consider the following sequences:

$$\begin{aligned} \left\{\binom{n}{2}\right\} &: \quad \{0\ \mathbf{0}\ 1\ 1\ 0\ 0\ 1\ 1\ \ldots\} \\ \left\{\binom{n}{2} + \binom{n}{1}\right\} &: \quad \{\mathbf{0}\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ \ldots\} \end{aligned} \tag{25}$$

Both sequences $\{\binom{n}{2}\}$ and $\{\binom{n}{2} + \binom{n}{1}\}$ are the same, but starting in different positions. We can check that the starting point of the sequence $\{\binom{n}{2} + \binom{n}{1}\}$ (bit in bold) is the second bit of sequence $\{\binom{n}{2}\}$.

In order to prove the linear complexity of the binomial sequences, we need to introduce the following results.

Proposition 11. *Given the binomial sequence* $\{\binom{n}{t}\}$, *with a fixed* $t \ge 1$, *the sequence represented by* $\{\binom{n}{t} + \binom{n}{t+1}\}$ *can be also represented by* $\{\binom{n}{t-1}\}$. *If* $t = 0$, *the sequence* $\{\binom{n}{t} + \binom{n}{t+1}\}$ *is the identically zero sequence.*

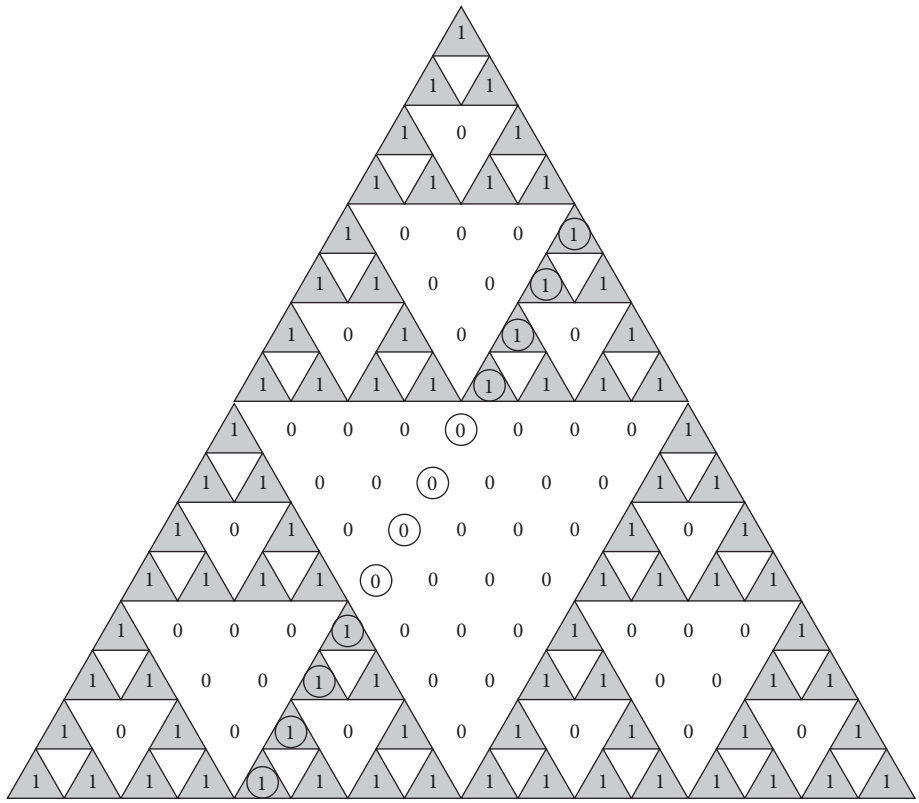


Figure 4: Binary Sierpinski's triangle where the circled bits correspond to the sequence $\{\binom{n}{4}\}$.

Proof. According to Lemma 8, we know that $\binom{n}{t} + \binom{n}{t-1} = \binom{n+1}{t}$. Since we are working over the binary field, we have that the sequence $\{\binom{n}{t} + \binom{n}{t+1}\}$ can be also represented by $\{\binom{n}{t-1}\}$. □

Theorem 12 ([13], Theorem 1). *Let $\{s_i\}_{i\geq 0}$ be a binary sequence whose characteristic polynomial is $(1+x)^n$. Then, the characteristic polynomial of the sequence $\{u_i\}_{i\geq 0}$, where $u_i = s_i + s_{i+1}$, is $(1+x)^{n-1}$.*

Now, we are ready to study the linear complexity of the binomial sequences.

Theorem 13. *The linear complexity of the sequence $\{\binom{n}{k}\}$ is $k+1$.*

Proof. We prove this result by induction.

For $k = 0$, the sequence $\{\binom{n}{0}\} = \{1\ 1\ 1\ 1\ 1\ \ldots\}$ has $LC_0 = 1$ and the characteristic polynomial is $(1+x)$.

For $k = 1$, the sequence $\{\binom{n}{1}\} = \{0\ 1\ 0\ 1\ \ldots\}$ represented by $\{\binom{n}{1}\}$ has $LC_1 = 2$ and the characteristic polynomial is $(1+x)^2$.

Let us suppose that the sequence $\{\binom{n}{k}\}$ has $LC_k = k+1$ and the characteristic polynomial is $(1+x)^{k+1}$.

According to Proposition 11, we have that $\{\binom{n}{k}\} = \{\binom{n}{k+1} + \binom{n+1}{k+1}\}$. Now, according to Theorem 12, the characteristic polynomial of $\{\binom{n}{k+1}\}$ is $(1+x)^{k+2}$ and, thus, $LC_{k+1} = k+2$. □

As a consequence of the previous theorem, we have the following result.

Corollary 14. *Given a sequence with binomial representation $\sum_{k=1}^{t}\{\binom{n}{i_k}\}$, where $i_1 < i_2 < \cdots < i_t$ are integer indices, then the linear complexity of such a sequence is $i_t + 1$.*

As a consequence of Lemma 9, we obtain the following result.

Theorem 15. *Let $\sum_{i=0}^{LC-1} c_i\{\binom{n}{i}\}$ with $c_i \in \mathbb{F}_2$ be the binomial representation of a sequence. If we shift cyclically such a sequence one bit to the left, then its binomial representation is*

$$\sum_{i=1}^{LC-1} c_i\left[\left\{\binom{n}{i} + \binom{n}{i-1}\right\}\right] + c_0\left\{\binom{n}{0}\right\}. \tag{26}$$

Corollary 16. *Binary sequences with period 2^L have 2^L different binomial representations.*

Proof. Since the period of the sequence is 2^L, we can perform 2^L left shifts before getting the same starting point of the sequence. Therefore, we can obtain 2^L different binomial representations. □

Example 17. Consider the sequence with binomial representation $\{\binom{n}{3} + \binom{n}{1}\}$. In Figure 5, we can see graphically the

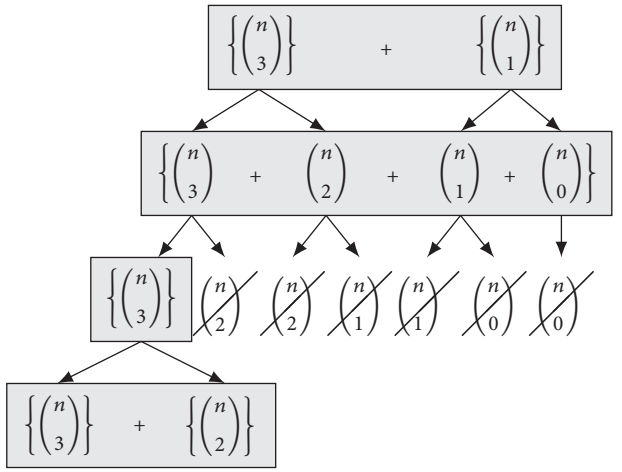


Figure 5: Binomial representations of the 4 shifted versions of the sequence $\{\binom{n}{3} + \binom{n}{1}\}$.

Table 2: Rules 102 and 60.

(a) *Rule 102:* $x_i^{t+1} = x_i^t + x_{i+1}^t$

111	110	101	100	011	010	001	000
0	1	1	0	0	1	1	0

(b) *Rule 60:* $x_i^{t+1} = x_{i-1}^t + x_i^t$

111	110	101	100	011	010	001	000
0	0	1	1	1	1	0	0

method followed to obtain the different binomial representations of this sequence. From one representation and via Theorem 15, we obtain the next representation corresponding to the same sequence left-shifted one bit. Finally, we have 4 different representations (the ones in bold contained in the grey boxes) including the initial one:

$$\begin{gathered}\left\{\binom{n}{3} + \binom{n}{1}\right\},\\ \left\{\binom{n}{3} + \binom{n}{2} + \binom{n}{1} + \binom{n}{0}\right\},\\ \left\{\binom{n}{3}\right\},\\ \left\{\binom{n}{3} + \binom{n}{2}\right\}.\end{gathered} \tag{27}$$

Since the period of this sequence is 4, we can obtain 4 different binary representations. Furthermore, one can observe that after four steps we obtain again the initial representation $\{\binom{n}{3} + \binom{n}{1}\}$.

Now, consider again Figure 4. We know that the binomial sequence $\{\binom{n}{4}\}$ showed in the binary Sierpinski's triangle starts in a different bit compared with the sequence $\{\binom{n}{4}\}$ given in Table 1. In particular, in the binary Sierpinski's triangle the sequences start in the first nonzero bit; thus their binomial representations are different. For instance, consider Table 3 where we can observe the different representations of a unique binomial sequence $\{\binom{n}{15}\}$. Each row represents the coefficients $\{c_0, c_1, \ldots, c_{15}\}$ of each different binomial representation. The binomial representation of the sequence $\{\binom{n}{15}\}$ in the binary Sierpinski's triangle is the last row of Table 3: $\sum_{i=0}^{15} c_i \{\binom{n}{i}\}$, with $c_i = 1$, for $i = 0, 1, \ldots, 15$.

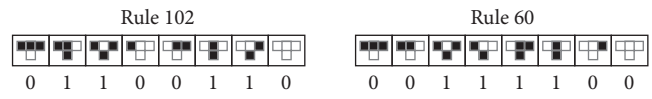


Figure 6: Rules 102 and 60 depicted in Wolfram's notation.

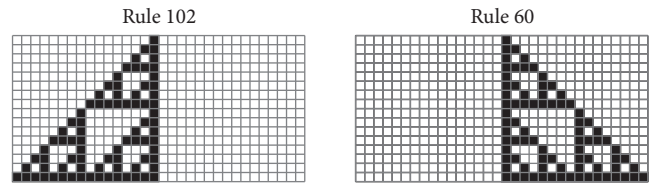


Figure 7: CA-images generated with rules 102 and 60.

5. Cellular Automata

Cellular automata (CA) are discrete structures composed of a finite number of cells whose content is updated according to a *rule* or function with k variables [14]. The state of the cell in position i at time $t + 1$, notated x_i^{t+1}, depends on the state of the k neighbour cells at time t. If these rules are composed exclusively of XOR operations, then the CA are *linear*. Here, the CA we consider are *regular* (every cell follows the same rule), *cyclic* (extreme cells are adjacent), and one-dimensional. For $k = 3$, rules 102 and 60 are given in Table 2.

The number 01100110 (00111100) is the binary representation of the decimal number 102 (60). In Figure 6, these rules are depicted according to Wolfram terminology [15]: a white square represents the digit 0 and a black square represents the digit 1.

Consider again Table 3. If we color the 1s, the general structure of the set of characterizations is the same as that one of the CA-image generated by rule 102 after having applied 15 iterations to the one-dimensional cellular automata (see Figure 7). In general, due to the observed form of the binomial sequences (see Figure 8 and Proposition 3), it can be assured that the complete set of binomial representations of $\{\binom{n}{2^L-1}\}$ coincides with the 102-CA of length and 2^L and initial state $\{0\ 0\ \ldots\ 0\ 1\}$. This is due to the fact that the recursive method to obtain the different binomial representations of a sequence matches with the generation rule of 102-CA (depicted in Table 2).

As a consequence, we can introduce the following result.

Theorem 18. *Consider a sequence* $\{u_j\}_{j\geq 0}$ *with binomial representation* $\sum_{i=0}^{LC-1} c_i \{\binom{n}{i}\}$. *If we put this sequence in the*

Table 3: Binomial representations of the 16 shifted versions of $\{\binom{n}{15}\}$.

$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$	$\binom{n}{5}$	$\binom{n}{6}$	$\binom{n}{7}$	$\binom{n}{8}$	$\binom{n}{9}$	$\binom{n}{10}$	$\binom{n}{11}$	$\binom{n}{12}$	$\binom{n}{13}$	$\binom{n}{14}$	$\binom{n}{15}$
c_0	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}	c_{12}	c_{13}	c_{14}	c_{15}
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1
0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1
0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	1
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1
0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	1
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

leftmost column of a 102-CA (rightmost column of a 60-CA), then the binomial representation of the next sequence $\{u_j + u_{j+1}\}_{j\geq 0}$ *in the CA is*

$$\sum_{i=0}^{LC-2} c_{i+1} \left\{\binom{n}{i}\right\}. \tag{28}$$

Proof. Let us denote the binomial sequence $\{\binom{n}{i}\}$ by $\{b_n^i\}_{n\geq 0}$. Then, we have that

$$u_j = \sum_{i=0}^{LC-1} c_i b_j^i, \quad j \geq 0$$

$$u_j + u_{j+1} = \sum_{i=0}^{LC-1} c_i b_j^i + \sum_{i=0}^{LC-1} c_i b_{j+1}^i = \sum_{i=0}^{LC-1} c_i \left(b_j^i + b_{j+1}^i\right), \tag{29}$$

$$j \geq 0.$$

According to Proposition 11,

$$u_j + u_{j+1} = \sum_{i=1}^{LC-1} c_i b_j^{i-1} = \sum_{k=0}^{LC-2} c_{k+1} b_j^k \tag{30}$$

Then, $\{u_j + u_{j+1}\}_{j\geq 0}$ is represented by $\sum_{i=0}^{LC-2} c_{i+1} \{\binom{n}{i}\}$. □

Remark 19. If the term $\binom{n}{0}$ is included in the binomial representation, it is discarded for the next sequence. See, for example, Table 4. In this table, we have two examples of one-dimensional linear CAs. The first one is a 102-CA. At the bottom of the CA, we can observe the binomial representations of the generated vertical sequences. We can check that the binomial representations of the sequences can be obtained following the process mentioned in Theorem 18. It is worth noticing that the given 60-CA generates exactly the same sequences, but they appear in reverse order.

Finally, observe that the set of binomial representations of a sequence follows the same pattern as the 102-CA.

Theorem 20 ([13], Theorem 4). *Given a sequence with period* 2^L *and linear complexity LC, then the CA that generates this sequence using the rule 102 has*

(i) *one sequence of period 1 (the identically 1 sequence),*

(ii) 2^{i-1} *sequences of period* 2^i*, for* $1 \leq i \leq L-2$,

(iii) $\mathrm{LC} - 2^{L-2}$ *sequences of period* 2^{L-1}.

Consider, for example, the sequence represented by $\{\binom{n}{0} + \binom{n}{2} + \binom{n}{3} + \binom{n}{5} + \binom{n}{12}\}$. This sequence has period $T = 16$. In Table 5, we can observe the 16 different representations of this sequence. The rows of the table represent the coefficients $\{c_0, c_1, \ldots, c_{12}\}$ that accompany each binomial coefficient, for each representation. That means, the column j represents the coefficients that accompany $\{\binom{n}{j}\}$ for each one of the 16 representations.

If we observe the behavior of the coefficients in the columns, we can check that the columns follow the same structure proposed in Theorem 20:

(i) One sequence of period 1 (rightmost sequence).

(ii) One sequences of period 2.

(iii) Two sequences of period 4.

(iv) Four sequences of period 8.

(v) Five sequences of period 16.

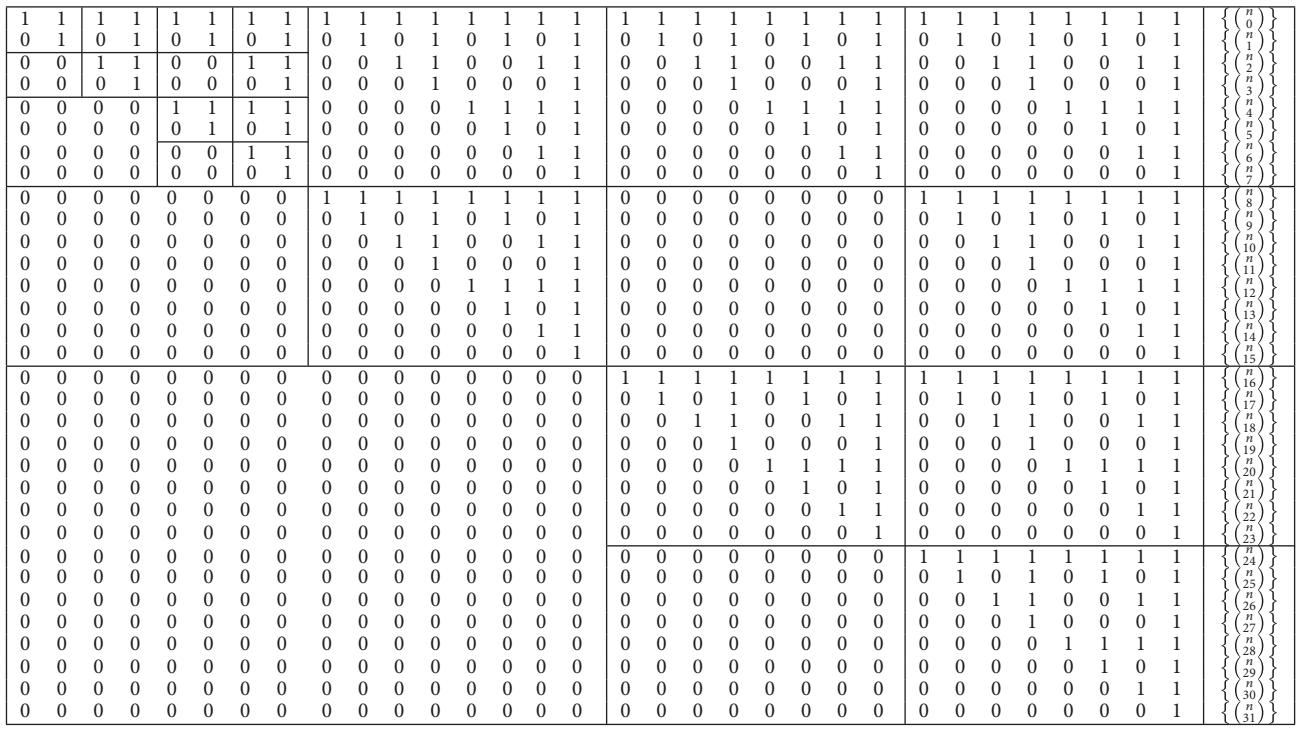


Figure 8: The first 32 binomial sequences.

Table 4: Examples of 102-CA and 60-CA and the binomial representation of the generated vertical sequences.

(a)

102	102	102	102	102
0	0	1	0	1
0	1	1	1	1
1	0	0	0	1
1	0	0	1	1
1	0	1	0	1
1	1	1	1	1
0	0	0	0	1
0	0	0	1	1
$\left\{\binom{n}{4}+\binom{n}{2}\right\}$	$\left\{\binom{n}{3}+\binom{n}{1}\right\}$	$\left\{\binom{n}{2}+\binom{n}{0}\right\}$	$\left\{\binom{n}{1}\right\}$	$\left\{\binom{n}{0}\right\}$

(b)

60	60	60	60	60
1	0	1	0	0
1	1	1	1	0
1	0	0	0	1
1	1	0	0	1
1	0	1	0	1
1	1	1	1	1
1	0	0	0	0
1	1	0	0	0
$\left\{\binom{n}{0}\right\}$	$\left\{\binom{n}{1}\right\}$	$\left\{\binom{n}{2}+\binom{n}{0}\right\}$	$\left\{\binom{n}{3}+\binom{n}{1}\right\}$	$\left\{\binom{n}{4}+\binom{n}{2}\right\}$

Table 5: Binomial representations of the 16 shifted versions of the sequence $\{\binom{n}{0} + \binom{n}{2} + \binom{n}{3} + \binom{n}{5} + \binom{n}{12}\}$.

$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$	$\binom{n}{5}$	$\binom{n}{6}$	$\binom{n}{7}$	$\binom{n}{8}$	$\binom{n}{9}$	$\binom{n}{10}$	$\binom{n}{11}$	$\binom{n}{12}$
c_0	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}	c_{12}
1	0	1	1	0	1	0	0	0	0	0	0	1
1	1	0	1	1	1	0	0	0	0	0	1	1
0	1	1	0	0	1	0	0	0	0	1	0	1
1	0	1	0	1	1	0	0	0	1	1	1	1
1	1	1	1	0	1	0	0	1	0	0	0	1
0	0	0	1	1	1	0	1	1	0	0	1	1
0	0	1	0	0	1	1	0	1	0	1	0	1
0	1	1	0	1	0	1	1	1	1	1	1	1
1	0	1	1	1	1	0	0	0	0	0	0	1
1	1	0	0	0	1	0	0	0	0	0	1	1
0	1	0	0	1	1	0	0	0	0	1	0	1
1	1	0	1	0	1	0	0	0	1	1	1	1
0	1	1	1	1	1	0	0	1	0	0	0	1
1	0	0	0	0	1	0	1	1	0	0	1	1
1	0	0	0	1	1	1	0	1	0	1	0	1
1	0	0	1	0	0	1	1	1	1	1	1	1
$T = 16$	$T = 16$	$T = 16$	$T = 16$	$T = 16$	$T = 8$	$T = 8$	$T = 8$	$T = 8$	$T = 4$	$T = 4$	$T = 2$	$T = 1$

Furthermore, it is possible to check that Table 5 is a 102-CA. This is due to the formation rule of the binomial representations given in (26), which coincides with the formation procedure of Rule 102.

6. Recovering the Binomial Representation

Given t intercepted bits of a sequence of period 2^L, Algorithm 1 introduces a method to recover a part of the binomial representation of such a sequence depending on the number t. Let us denote by $\boldsymbol{s}$ the set of intercepted bits. In round j, the algorithm compares $\boldsymbol{s}_j$ with the corresponding bit in the sequence represented by $\sum_{i=0}^{j} \{\binom{n}{i}\}$. If they match, then $\{\binom{n}{j}\}$ is part of the binomial representation. Otherwise, the term $\{\binom{n}{j}\}$ is discarded and the algorithm continues. This method is based on the fact that the first j bits of the sequence represented by $\{\binom{n}{j}\}$ are 0s.

Let us introduce now an illustrative example.

Example 21. Consider the set of intercepted bits $\boldsymbol{s} = \{1\ 1\ 0\ 1\ 1\ 1\}$. The first two bits ($\boldsymbol{s}_0 = 1$ and $\boldsymbol{s}_1 = 1$) match with the first two bits of the sequence $\{\binom{n}{0}\} = \{\mathbf{1}\ \mathbf{1}\ 1\ 1\ \ldots\}$. This means that one of the binomial representations of the sequence starts with $\sum_{i=0}^{1} c_i \{\binom{n}{i}\} = \{\binom{n}{0}\}$ $(c_0 = 1, c_1 = 0)$.

The bit $\boldsymbol{s}_2 = 0$ matches with the corresponding bit of the sequence $\{\binom{n}{0} + \binom{n}{2}\}$:

$$\begin{array}{l} \left\{\binom{n}{0}\right\} : 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ \ldots \\ \left\{\binom{n}{2}\right\} : 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ \ldots \\ \hline 1\ 1\ \mathbf{0} \end{array} \tag{31}$$

Then, the binomial representation we are considering starts with $\sum_{i=0}^{2} c_i \{\binom{n}{i}\} = \{\binom{n}{0} + \binom{n}{2}\}$ $(c_0 = 1, c_1 = 0, c_2 = 1)$.

Finally, the bits $\boldsymbol{s}_3 = 1$, $\boldsymbol{s}_4 = 1$, and $\boldsymbol{s}_5 = 1$ match with the corresponding bits of the sequence $\{\binom{n}{0} + \binom{n}{2} + \binom{n}{3}\}$:

$$\begin{array}{l} \left\{\binom{n}{0}\right\} : 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ \ldots \\ \left\{\binom{n}{2}\right\} : 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ \ldots \\ \left\{\binom{n}{3}\right\} : 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ \ldots \\ \hline 1\ 1\ 0\ \mathbf{1}\ \mathbf{1}\ \mathbf{1} \end{array} \tag{32}$$

Therefore, we have that the first part of the considered binomial representation is $\sum_{i=0}^{5} c_i \{\binom{n}{i}\} = \{\binom{n}{0} + \binom{n}{2} + \binom{n}{3}\}$ with coefficients as in Table 6. In case of having more intercepted bits and proceeding in the same way, we would complete the whole representation.

Next, we introduce a result on the number of bits required to recover the binomial representation of a sequence. Notice that if we know the binomial representation of a sequence, we can recover the whole sequence.

Proposition 22. *Given $LC - 1$ intercepted bits of a sequence with linear complexity LC and period 2^L, it is possible to recover the complete the binomial representation of the sequence.*

Proof. According to Corollary 14, the binomial representation of a sequence with linear complexity LC and period 2^L is of the form $\sum_{i=0}^{LC-1} c_i \{\binom{n}{i}\}$, with $c_{LC-1} = 1$. Now, according to the method explained in Algorithm 1, we need $LC - 1$ bits to recover each one of the coefficients c_i, $i = 0, 1, \ldots, LC-1$. □

Table 6: Coefficients in Example 21.

c_0	c_1	c_2	c_3	c_4	c_5
1	0	1	1	0	0

Input:
$\boldsymbol{s}$: Intercepted bits
01: $\boldsymbol{repr}$ = {0 0 0 0 ... };
02: $t = length(\boldsymbol{v})$;
03: **for** j = 0 **to** $t - 1$ **do**
04: **if** $\boldsymbol{s}_j \neq \boldsymbol{repr}_j$ then
05: $\boldsymbol{repr} = \boldsymbol{repr} + \binom{n}{j}$;
06: **endif**
07: **endfor**
Output:
$\boldsymbol{repr}$: Binomial representation of the intercepted bits

Algorithm 1: Constructing the binomial representation of a given sequence.

At any rate, the application of the traditional Berlekamp-Massey algorithm [16] needs $2 \cdot LC$ intercepted bits to recover the whole sequence. Thus, the method here developed makes use of half the bits needed by the Berlekamp-Massey algorithm. Consequently, the amount of intercepted bits has been reduced by a factor 2, which is quite favorable in terms of cryptanalysis.

7. Conclusions

The family of binary sequences considered in this work, sequences whose period is a power of 2, has good cryptographic properties such as long period and large linear complexity. However, we have seen that such sequences are simple solutions of linear difference equations with constant coefficients and can be obtained by XORing binomial binary sequences corresponding to diagonals of Sierpinski's triangle reduced modulo 2. Although different nonlinear procedures, e.g., irregular decimation, are introduced to break the linearity of the LFSR-based sequence generators, this linearity is still visible in their output sequences. Consequently, such linearity makes the generators producing the previous sequences vulnerable against cryptanalysis and makes them not suitable as part of more complex cryptographic structures. In this sense, we conjecture that given a sequence there exists a minimal binomial representation, that is, a representation with a minimum number of binomial terms.

On the other hand, we showed that there exists a close relation between one-dimensional linear cellular automata (102-CAs or 60-CAs) and the binomial sequences. Furthermore, there exists another family of cellular automata (150/90-CAs) that also generate sequences of period 2^L with good cryptographic properties. Therefore, in order to complete this study, the analysis of the relation of this family of cellular automata with binomial sequences is proposed as future work.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research has been partially supported by Ministerio de Economía, Industria y Competitividad (MINECO), Agencia Estatal de Investigación (AEI), and Fondo Europeo de Desarrollo Regional (FEDER, UE) under Project COPCIS, Reference TIN2017-84844-C2-1-R, and by Comunidad de Madrid (Spain) under Project Reference CYNAMON (P2018/TCS-4566) and also cofunded by European Union FEDER funds. The first author was supported by CAPES (Brazil). Finally, we would also like to thank Dr. Verónica Requena for her useful comments and suggestions.

References

[1] S. W. Golomb, *Shift Register-Sequences*, Aegean Park Press, Laguna Hill, California, USA, 1982.

[2] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, USA, 1996.

[3] W. Meier and O. Staffelbach, "The self-shrinking generator," in *Advances in cryptology -EUROCRYPT '94 (Perugia)*, A. De Santis, Ed., vol. 950 of *Lecture Notes in Computer Science*, pp. 205–214, Springer, Berlin, Heidelberg, Germany, 1995.

[4] Y. Hu and G. Xiao, "Generalized self-shrinking generator," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 50, no. 4, pp. 714–719, 2004.

[5] A. Kanso, "Modified self-shrinking generator," *Computers and Electrical Engineering*, vol. 36, no. 5, pp. 993–1001, 2010.

[6] S. D. Cardell and A. Fúster-Sabater, "The t-modified self-shrinking generator," in *Computational Science – ICCS 2018*, Y. Shi, H. Fu, and Y. Tian, Eds., vol. 10860 of *Lecture Notes in Computer Science*, pp. 653–663, Springer International Publishing, Cham, 2018.

[7] A. Fauré, A. Naldi, C. Chaouiya, and D. Thieffry, "Dynamical analysis of a generic Boolean model for the control of the mammalian cell cycle," *Bioinformatics*, vol. 22, no. 14, pp. e124–e131, 2006.

[8] D. Zheng, G. Yang, X. Li, Z. Wang, F. Liu, and L. He, "An efficient algorithm for computing attractors of synchronous and asynchronous boolean networks," *Plos One*, vol. 8, no. 4, Article ID e60593, 2013.

[9] J. A. Aledo, S. Martínez, and J. C. Valverde, "Graph dynamical systems with general boolean states," *Applied Mathematics Information Sciences*, vol. 9, no. 4, pp. 1803–1808, 2015.

[10] J. A. Aledo, S. Martínez, F. L. Pelayo, and J. C. Valverde, "Parallel discrete dynamical systems on maxterm and minterm boolean functions," *Mathematical and Computer Modelling*, vol. 55, no. 3-4, pp. 666–671, 2012.

[11] J. A. Aledo, S. Martínez, and J. C. Valverde, "Parallel dynamical systems over graphs and related topics: a survey," *Journal of Applied Mathematics*, vol. 2015, Article ID 594294, 14 pages, 2015.

[12] A. Fúster-Sabater and P. Caballero-Gil, "Linear cellular automata as discrete models for generating cryptographic sequences," *Journal of Research and Practice in Information Technology*, vol. 40, no. 4, pp. 47–52, 2008.

[13] S. D. Cardell and A. Fúster-Sabater, "Linear models for the self-shrinking generator based on CA," *Journal of Cellular Automata*, vol. 11, no. 2-3, pp. 195–211, 2016.

[14] A. K. Das, A. Ganguly, A. Dasgupta, S. Bhawmik, and P. P. Chaudhuri, "Efficient characterisation of cellular automata," *IEE Proceedings Part E Computers and Digital Techniques*, vol. 137, no. 1, pp. 81–87, 1990.

[15] S. Wolfram, "Cellular automata as simple self-organizing system," *Caltrech preprint CALT*, pp. 68–938, 1982.

[16] J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Transactions on Information Theory*, vol. 15, no. 1, pp. 122–127, 1969.